

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-301489

(43)Date of publication of application : 13.11.1998

(51)Int.Cl.

G09C 1/00
H04K 1/06
H04L 9/06

(21)Application number : 09-104634

(71)Applicant : TAISEI CORP

(22)Date of filing : 22.04.1997

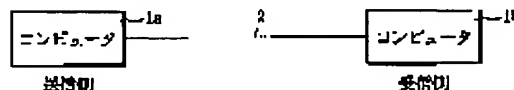
(72)Inventor : NOMURA KIYOSUKE

(54) DATA CONVERTER

(57)Abstract:

PROBLEM TO BE SOLVED: To reduce the cost, time and labour required to develop the ciphering/ deciphering software compact in size by dividing the prescribed area of data so that plural areas having a prescribed length are constituted and a pair of areas, which are combined employing a specific rule, and a similar pair of areas are exchanged.

SOLUTION: This converter is constituted of a computer 1a which ciphers plain data and transmits the data and a computer 1b which decipheres the received ciphered data. The computer 1a and 1b are connected by a data transmitting path 2. In the converter, plain data are divided into the areas having a prescribed length for the ciphering. Then, the divided areas are made into pairs with other areas by a specific combination and these areas are exchanged. On the other hand, during a deciphering, the ciphered data are divided into the areas having a prescribed length. Then, each area is made into a pair with another area employing the same combination used during the ciphering and these areas are exchanged.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-301489

(43)公開日 平成10年(1998)11月13日

(51)Int.Cl.⁶
G 0 9 C 1/00
H 0 4 K 1/06
H 0 4 L 9/06

識別記号
6 1 0

F I
G 0 9 C 1/00
H 0 4 K 1/06
H 0 4 L 9/00
6 1 0 A
6 1 1 Z

審査請求 未請求 請求項の数7 O L (全 12 頁)

(21)出願番号 特願平9-104634
(22)出願日 平成9年(1997)4月22日

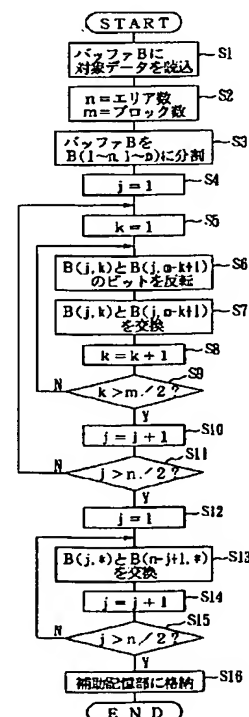
(71)出願人 000206211
大成建設株式会社
東京都新宿区西新宿一丁目25番1号
(72)発明者 野村 享右
東京都新宿区西新宿一丁目25番1号 大成
建設株式会社内
(74)代理人 弁理士 森 哲也 (外3名)

(54)【発明の名称】 データ変換装置

(57)【要約】

【課題】 暗号化／復号化ソフトを開発するために要する費用や時間、または手間などを大幅に削減するとともに、コンパクトなサイズの暗号化／復号化ソフトを開発することができるデータ変換装置を提供する。

【解決手段】 コンピュータの記憶手段に格納されているデータを、暗号化および復号化するデータ変換装置において、データの所定領域を所定長のエリアが複数個構成されるように分割するデータ分割手段と、特定の組み合わせで対にしたエリア同士を交換するエリア交換手段と、を備える。



【特許請求の範囲】

【請求項1】 コンピュータの記憶手段に格納されているデータを、暗号化及び復号化するデータ変換装置において、

データの所定領域を所定長のエリアが複数個構成されるように分割するデータ分割手段と、特定の組み合わせで対にした前記エリア同士を交換するエリア交換手段と、を備えることを特徴とするデータ変換装置。

【請求項2】 前記データ分割手段は、前記所定領域を前記エリアが偶数個構成されるように分割することを特徴とする請求項1記載のデータ変換装置。

【請求項3】 前記エリア交換手段は、前記すべてのエリアを必ず一度だけ交換する単位交換処理を、少なくとも1回実行することを特徴とする請求項2記載のデータ変換装置。

【請求項4】 前記データ分割手段は、さらに前記エリアを所定長のブロックが複数個構成されるように分割するブロック分割処理を、前記すべてのエリアについて等しく実行し、前記エリア交換手段は、同一エリア内で特定の組み合わせで対にした前記ブロック同士を交換するブロック交換処理を、前記すべてのエリアについて等しく実行することを特徴とする請求項1、2又は3記載のデータ変換装置。

【請求項5】 前記データ分割手段は、前記エリアを前記ブロックが偶数個構成されるように分割することを特徴とする請求項4記載のデータ変換装置。

【請求項6】 データの前記所定領域を構成するビットを反転するビット反転手段を備えることを特徴とする請求項1、2、3、4又は5記載のデータ変換装置。

【請求項7】 前記エリアを対にする組み合わせを特定するための特定キーを入力する特定キー入力手段を備え、前記エリア交換手段は、特定キー入力手段から入力された特定キーに基づいて前記各エリアを対にすることを特徴とする請求項1、2又は6記載のデータ変換装置。

【発明の詳細な説明】

【0001】

【発明の属する技術の分野】 本発明は、データを暗号化および復号化するデータ変換装置に係り、特に、暗号化データを生成するときと同一の処理で、その暗号化データを復号化することのできるデータ変換装置に関する。

【0002】

【従来の技術】 従来のデータ変換装置としては、通信データの盗聴、改ざんなどの不正アクセスから通信データを保護するために用いられる暗号化技術がある。これには、例えば、ソフトウェアを利用してデータを暗号化および復号化するものがあり、次のようにしてデータの送受信を行う。

【0003】 送信元コンピュータでは、データを送信しようとする送信者が暗号化ソフトを利用し、送信対象と

なる平文データを、送信者によって指定された所定の暗号キーに基づいて暗号化し、その暗号化データを送信する。

【0004】 このとき、例えば、DES (Data Encryption Standard) 方式によってデータを暗号化する暗号化ソフトは、図8 (a) に示すように、平文データを暗号化するデータ処理部と、指定された暗号キーから暗号化するために必要なキー情報系列を生成するキースケジューラ部とで構成されている。データ処理部では、64ビットごとに平文データを分割し、分割したデータ列をキースケジューラ部で生成されたキー情報系列を用い、同一の変換を16段繰り返して64ビットの暗号化データを生成する。一方、キースケジューラ部では、64ビットで構成される暗号キーを用いて16段のキー情報系列 K_1 、 K_2 、…、 K_{16} を生成する。なお、図中、 f は、図8 (b) に示すように、非線形変換であって、6ビット入力4ビット出力のテーブルで与えられる8個のSボックスからなっている。

【0005】 一方、送信先コンピュータでは、データを受信した受信者が復号化ソフトを利用し、受信した暗号化データを、受信者によって指定された所定の復号キーに基づいて復号化する。

【0006】 このとき、例えば、DES方式によってデータを復号化する復号化ソフトは、図8 (a) において、キースケジューラ部で生成するキー情報系列を暗号化したときとは逆に、 K_{16} 、 K_{15} 、…、 K_1 とすれば、元の平文データが得られる。ただし、受信者が指定した復号キーと送信者が指定した暗号キーとが一致しなければ、元の平文データを得ることができない。

【0007】

【発明が解決しようとする課題】 しかしながら、従来のデータ変換装置は、暗号化するときのキー情報系列に対して、復号化するときのキー情報系列を逆の順序で生成する必要があるため、暗号化するためのデータ処理部と復号化するためのデータ処理部とを個別に設計しなければならなかった。

【0008】 このため、従来、暗号化／復号化ソフトを開発する際には、暗号化または復号化するためのデータ処理部をそれぞれ個別に設計する必要があること、また、暗号化データ処理部で生成された暗号化データを、復号化データ処理部で確実に復号化することができるかを厳密にテストする必要があることなどから、費用や時間や手間などがかかるとともに、完成するソフトのデータ容量も大きなものになってしまう。

【0009】 そこで、本発明は、このような従来の問題を解決することを課題としており、暗号化データを生成するときと同一の処理で、その暗号化データを復号化することによって、暗号化／復号化ソフトを開発するために要する費用や時間、または手間などを大幅に削減するとともに、コンパクトなサイズの暗号化／復号化ソフト

を開発することのできるデータ変換装置を提供することを目的としている。

【0010】

【課題を解決するための手段】上記目的を達成するために、本発明に係る請求項1記載のデータ変換装置は、コンピュータの記憶手段に格納されているデータを、暗号化および復号化するデータ変換装置において、データの所定領域を所定長のエリアが複数個構成されるように分割するデータ分割手段と、特定の組み合わせで対にした前記エリア同士を交換するエリア交換手段と、を備えることを特徴としている。

【0011】このような構成であれば、平文データを暗号化するときには、暗号化しようとする平文データは、データ分割手段で、所定長のエリアに分割される。そうして、分割された各エリアは、エリア交換手段で、特定の組み合わせで他のエリアと対にされ、それらエリア同士が交換される。したがって、平文データは、分割したエリアの配置が拡散されるので、解読困難な暗号化データに暗号化される。

【0012】なお、このとき、エリアの長さは、エリアが複数個構成されるように、平文データの長さに応じて決定してもよいし、また逆に、エリアの長さをあらかじめ決定しておき、平文データにダミーデータを付加することによって、エリアが複数個構成されるように調整してもよい。

【0013】一方、暗号化データを復号化するときには、暗号化データは、データ分割手段で、前記所定長のエリアに分割される。そうして、各エリアは、エリア交換手段で、暗号化したときと同一の組み合わせで他のエリアと対にされ、それらエリア同士が交換される。したがって、暗号化データは、エリアの配置が初期の状態に戻されるため、解読可能な元の平文データに復号化される。

【0014】なお、ここで、平文データまたは暗号化データは、部分的に暗号化または復号化してもよく、そのような場合には、平文データのうち暗号化しようとする領域を、前記所定長のエリアが複数個構成されるように分割する。ただし、暗号化したときの暗号化領域と、復号化するときの復号化領域とを一致させなければならない。

【0015】端的にいえば、暗号化データを生成するときと同一の処理で、その暗号化データを復号化するには、平文データを暗号化データに変換する写像関数と、暗号化データを平文データに変換する写像関数とが逆関数の関係にある必要がある。したがって、一のエリアを任意の位置に移動させた場合には、移動先にある他のエリアを、その一のエリアが配置されていた位置に移動することが条件となる。この条件を満たすには、各エリアを対にして交換すればよい。

【0016】これには、例えば、先頭と末尾とから計数

して同一番目に属するエリアを対にし、それらエリア同士を交換するような場合が挙げられる。そうすると、先頭にあるエリアほど末尾に移動させられるので、結果として、変換されたエリアの配置は、元のエリアの配置と逆順となる。

【0017】また、本発明に係る請求項2記載のデータ変換装置は、請求項1記載のデータ変換装置において、前記データ分割手段は、前記所定領域を前記エリアが偶数個構成されるように分割することを特徴としている。

【0018】このような構成であれば、平文データまたは暗号化データは、データ分割手段で、エリアが偶数個構成されるように分割される。したがって、分割された各エリアは、必ず他のエリアと対にされて交換される。

【0019】さらに、本発明に係る請求項3記載のデータ変換装置は、請求項2記載のデータ変換装置において、前記エリア交換手段は、前記すべてのエリアを必ず一度だけ交換する単位交換処理を、少なくとも1回実行することを特徴としている。

【0020】このような構成であれば、各エリアは、1回の単位交換処理において、対となる他のエリアと必ず1度だけ交換される。そうして、この単位交換処理が1または複数回実行される。

【0021】ここで、単位交換処理を複数回実行するときには、各単位交換処理ごとに対するエリアの組み合わせを異ならせることが望ましい。この場合において、組み合わせを異ならせたとしても、単位交換処理でエリアを交換するようにすれば、最初のエリアの配置から複数回の単位交換処理を経て得られたエリアの配置への変換が上記逆関数の関係を満たしているため、例えば、平文データを、異なる複数の単位交換処理A、B、Cの順序で暗号化したときであっても、その暗号化データは、単位交換処理A、B、Cの順序で元の平文データに復号化することができる。

【0022】また、単位交換処理を含む上記処理を応用した暗号化／復号化ソフトを開発する際には、エリアの分割個数を大きく設定すればするほど、処理パターンを幅広く選択することができる。このため、これらの処理パターンを適宜に組み合わせ、例えば、データの複数の領域について異なる処理パターンで暗号化するなどすれば、バリエーションに富んだソフトを開発することができる。また逆に、このように多数の処理パターンが存在することに着目して、あらかじめいくつかの処理パターンを登録しておき、それら処理パターンのいずれかを指定するようなものを暗号キー／復号キーとして用いることも考えられる。

【0023】さらに、本発明に係る請求項4記載のデータ変換装置は、請求項1、2または3記載のデータ変換装置において、前記データ分割手段は、さらに前記エリアを所定長のブロックが複数個構成されるように分割するブロック分割処理を、前記すべてのエリアについて等

しく実行し、前記エリア交換手段は、同一エリア内で特定の組み合わせで対にした前記ブロック同士を交換するブロック交換処理を、前記すべてのエリアについて等しく実行することを特徴としている。

【0024】このような構成であれば、各エリアは、さらに複数のブロックに分割されるが、すべてのエリアにおいて、各エリアごとに構成されるブロックの個数が同数となるように分割される。そうして、エリア内の各ブロックは、特定の組み合わせで他のブロックと対にされて交換されるが、すべてのエリアにおいて、各ブロックが同一の組み合わせで対にされて交換される。

【0025】この請求項4記載の発明において、特定の組み合わせとは、請求項1記載の発明における特定の組み合わせと同一の組み合わせであってもよいし、異なる組み合わせであってもよい。

【0026】さらに、本発明に係る請求項5記載のデータ変換装置は、請求項4記載のデータ変換装置において、前記データ分割手段は、前記エリアを前記ブロックが偶数個構成されるように分割することを特徴としている。

【0027】このような構成であれば、各エリアは、データ分割手段で、ブロックが偶数個構成されるように分割される。したがって、分割された各ブロックは、必ず他のブロックと対にされて交換される。

【0028】さらに、本発明に係る請求項6記載のデータ変換装置は、請求項1、2、3、4または5記載のデータ変換装置において、データの前記所定領域を構成するビットを反転するビット反転手段を備えることを特徴としている。

【0029】このような構成であれば、平文データを暗号化するときには、その平文データは、ビット反転手段で、構成するビットが反転されて読解困難な暗号化データに暗号化されるが、暗号化データを復号化するときには、その暗号化データは、反転されたビットがさらに反転されて元の平文データに復号化される。このとき、構成するすべてのビットを反転する必要はなく、特定のビットのみを反転するようにしてもよい。

【0030】さらに、本発明に係る請求項7記載のデータ変換装置は、請求項1、2または6記載のデータ変換装置において、前記エリアを対にする組み合わせを特定するための特定キーを入力する特定キー入力手段を備え、前記エリア交換手段は、特定キー入力手段から入力された特定キーに基づいて前記各エリアを対にすることを特徴としている。

【0031】このような構成であれば、分割された各エリアは、エリア交換手段で、特定キー入力手段から入力された特定キーによって特定される組み合わせに基づいて、他のエリアと対にされ、それらエリア同士が交換される。

【0032】したがって、暗号化データを生成するとき

に入力した特定キーと、その暗号化データを復号化しようとするときに入力する特定キーとが一致しなければ、その暗号化データは、元の平文データに復号化されない。

【0033】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照しながら説明する。図1は、本発明に係るデータ変換装置の第1の実施の形態を示す概略構成図である。図2は、図1におけるコンピュータの構成を示すブロック図である。

【0034】この第1の実施の形態は、本発明に係るデータ変換装置を、図1に示すように、2台のコンピュータ間で、平文データを暗号化して送受信する場合について適用したものである。

【0035】このデータ変換装置は、平文データを暗号化して送信するコンピュータ1aと、受信した暗号化データを復号化するコンピュータ1bとで構成されており、コンピュータ1aとコンピュータ1bとは、暗号化データを伝送するためのデータ伝送路2で接続されている。

【0036】同一機能を有する各コンピュータ1a、1bは、図2に示すように、演算およびシステム全体を制御する演算処理部3と、データの読み出しおよび書き込みが可能な主記憶部4および補助記憶部5と、外部からデータ入力可能なヒューマンインターフェースとしてのキーボード6と、キーボード6からデータを入力し、かつ、データ伝送路2を介して他方のコンピュータと暗号化データの入出力を行うインターフェース部7とで構成されており、演算処理部3、主記憶部4、補助記憶部5およびインターフェース部7は、データを伝送するためのバスで相互に接続されている。

【0037】主記憶部4は、ROMおよびRAM等の記憶素子からなり、あらかじめ演算処理部3の制御プログラム等が格納されており、補助記憶部4から読み込んだデータおよび演算処理部3の演算過程に必要な演算結果を格納するように構成されている。

【0038】補助記憶部5は、ハードディスク等からなり、暗号化しようとする平文データ、または、復号化しようとする暗号化データを格納するように構成されている。演算処理部3は、マイクロプロセッサユニットMPU等からなり、補助記憶部5に格納されている平文データを暗号化し、または、暗号化データを復号化しようとするときには、主記憶部4に格納されている所定のプログラムを起動させ、図3のフローチャートに示す処理を実行するように構成されている。ここで、図3は、平文データを暗号化し、または、暗号化データを復号化するための処理を示すフローチャートである。

【0039】つまり、平文データを暗号化し、または、暗号化データを復号化しようとするときに、演算処理部3では、次のようにして処理を実行する。まず始めに、

図3に示すように、ステップS1に移行して、データを格納するためのバッファBに補助記憶部5から処理対象となる対象データを読み込み、ステップS2に移行して、変数nに偶数の値をとるエリア数を、変数mに偶数の値をとるブロック数を設定し、ステップS3に移行して、バッファBを変数nが示す個数のエリアに分割し、さらに、各エリアを変数mが示す個数のブロックに分割する。ここで、変数nに設定するエリア数および変数mに設定するブロック数は、あらかじめ設定した固定の値を用いるものとする。

【0040】すなわち、バッファBに読み込んだ対象データは、エリアが変数nが示す個数だけ構成されるように分割され、さらに、各エリアは、ブロックが変数mが示す個数だけ構成されるように分割される。このとき、エリアの長さは、対象データの長さを変数nが示す値で除した値で決定され、ブロックの長さは、同様に、エリアの長さを変数mが示す値で除した値で決定される。

【0041】なお、以降、対象データの先頭からj ($1 \leq j \leq n$) 番目のエリアにおいて、そのエリアの先頭からk ($1 \leq k \leq m$) 番目のブロックに格納されているデータを示す場合には、B(j, k)と、j番目のエリアにおいて、すべてのブロックに格納されているデータを示す場合には、B(j, *)と表記する。

【0042】次いで、ステップS4に移行して、処理回数を計数するための変数jに“1”を設定し、ステップS5に移行して、処理回数を計数するための変数kに“1”を設定し、ステップS6に移行して、バッファB(j, k)とバッファB(j, m-k+1)とに格納されているデータを構成するすべてのビットを反転し、ステップS7に移行して、バッファB(j, k)に格納されているデータとバッファB(j, m-k+1)に格納されているデータとを交換する。そうすると、バッファB(j, k)には、バッファB(j, m-k+1)に格納されていたデータを構成するすべてのビットが反転されたものが格納され、バッファB(j, m-k+1)には、バッファB(j, k)に格納されていたデータを構成するすべてのビットが反転されたものが格納される。

【0043】次いで、ステップS8に移行して、変数kの値に“1”を加算し、ステップS9に移行して、変数kの値が変数mの半値より大きいかなんかを判定し、大きいと判定されたときには、ステップS10に移行するが、大きくないと判定されたときには、ステップS6に移行する。

【0044】すなわち、ステップS5からステップS9までは、変数kの値が“1”ずつ増加していくので、j番目のエリアにおいて、そのエリアの半分の位置を対称にして各ブロックが先頭から順次交換されることになる。

【0045】ステップS10では、変数jの値に“1”を加算し、ステップS11に移行して、変数jの値が変

数nの半値より大きいかなんかを判定し、大きいと判定されたときには、ステップS12に移行するが、大きくないと判定されたときには、ステップS5に移行する。

【0046】すなわち、ステップS4からステップS11までは、変数jの値が“1”ずつ増加していくので、すべてのエリアについて、ステップS5からステップS9までの処理が実行されることになる。

【0047】ステップS12では、変数jに“1”を設定し、ステップS13に移行して、バッファB(j, *)に格納されているデータとB(n-j+1, *)に格納されているデータとを交換し、ステップS14に移行して、変数jの値に“1”を加算し、ステップS15に移行して、変数jの値が変数nの半値より大きいかなんかを判定し、大きいと判定されたときには、ステップS16に移行するが、大きくないと判定されたときには、ステップS13に移行する。

【0048】すなわち、ステップS12からステップS15までは、変数jの値が“1”ずつ増加していくので、対象データの半分の位置を対称にして各エリアが先頭から順次交換されることになる。

【0049】そうして、ステップS16では、このように対象データのエリアの配置を拡散したものを、補助記憶部5の所定領域に格納して、一連の処理を終了する。次に、上記第1の実施の形態の動作を図面を参照しながら説明する。図4は、平文データを暗号化する場合を説明するブロック図である。図5は、暗号化データを復号化する場合を説明するブロック図である。

【0050】始めに、コンピュータ1aの補助記憶部5に格納されている平文データを暗号化して、その暗号化データをコンピュータ2bに送信する場合について説明する。

【0051】まず、データを送信しようとする送信者は、ステップS1において、送信対象となる平文データをバッファBに読み込む。そうすると、ステップS2からS3までを経て、バッファBに格納された平文データは、図4(a)に示すように、エリアが変数nが示す個数(例えば、N個)構成されるように分割され、さらに、各エリアは、ブロックが変数mが示す個数(例えば、M個)構成されるように分割される。このとき、B(1, *)には、データD₁が格納されており、B(j, 1~M)には、データd₁~d_Mが格納され、B(N-j+1, *)には、データD_{N-j+1}が格納され、B(N, *)には、データD_Nが格納されているものとする。

【0052】次いで、ステップS4からS11までを経て、各エリア内において、その各ブロックに格納されているデータは、構成するすべてのビットが反転されるとともに、そのエリアの半分の位置M/2を対称にして交換される。例えば、図4(b)に示すように、j番目のエリアであるB(j, *)では、まず、そのエリアの先

頭にあるデータ d_1 と末尾にあるデータ d_M とが交換され、次に、先頭から2番目にあるデータ d_2 と末尾から2番目にあるデータ d_{M-1} とが交換され、次に、データ d_3 とデータ d_{M-2} とが、データ d_4 とデータ d_{M-3} とが交換されていく。

【0053】したがって、 $B(1, *)$ には、データ D_1 内のブロックが交換されたデータ $/D_1$ が格納され、 $B(j, 1 \sim M)$ には、データ $d_M \sim d_1$ が格納され、 $B(N-j+1, *)$ には、データ D_{N-j+1} 内のブロックが交換されたデータ $/D_{N-j+1}$ が格納され、 $B(N, *)$ には、データ D_N 内のブロックが交換されたデータ $/D_N$ が格納される。なお、ここで、“/”は、エリア内のブロックが交換された状態のデータを示すための表記である。

【0054】次いで、ステップS12からS15までを経て、各エリアに格納されているデータは、平文データの半分の位置 $N/2$ を対称にして交換される。例えば、図4(c)に示すように、まず、平文データの先頭にあるデータ $/D_1$ と末尾にあるデータ $/D_N$ とが交換され、先頭から j 番目にあるデータ $d_M \sim d_1$ と末尾から j 番目にあるデータ $/D_{N-j+1}$ とが交換されていく。

【0055】したがって、 $B(1, *)$ には、データ $/D_N$ が格納され、 $B(j, *)$ には、データ $/D_{N-j+1}$ が格納され、 $B(N-j+1, 1 \sim M)$ には、データ $d_M \sim d_1$ が格納され、 $B(N, *)$ には、データ $/D_1$ が格納される。

【0056】すなわち、この平文データは、エリアの配置が拡散されるので、解読困難な暗号化データとなり、ステップS16において、補助記憶部5の所定領域に格納される。そうして、送信者は、この暗号化データをデータ伝送路2を介して、コンピュータ1bに送信する。

【0057】次に、コンピュータ1bにおいて、コンピュータ1aから送信された暗号化データを復号化する場合について説明する。まず、データ伝送路2を介して送信された暗号化データは、インターフェース部7で受信され、補助記憶部5の所定領域に格納される。

【0058】次いで、この暗号化データを受信した受信者は、ステップS1において、復号化しようとするその暗号化データをバッファBに読み込む。そうすると、ステップS2からS3までを経て、バッファBに格納された暗号化データは、図5(a)に示すように、平文データを暗号化したときと同様に、エリアが N 個構成されるように分割され、さらに、各エリアは、ブロックが M 個構成されるように分割される。このとき、平文データを分割したときと同一のエリア長およびブロック長で暗号化データを分割するので、 $B(1, *)$ には、データ $/D_N$ が格納され、 $B(j, *)$ には、データ $/D_{N-j+1}$ が格納され、 $B(N-j+1, 1 \sim M)$ には、データ $d_M \sim d_1$ が格納され、 $B(N, *)$ には、データ $/D_1$ が格納されていることになる。

【0059】次いで、ステップS4からS11までを経て、各エリア内において、その各ブロックに格納されているデータは、構成するすべてのビットが反転されるとともに、そのエリアの半分の位置 $M/2$ を対称にして交換される。

【0060】したがって、図5(b)に示すように、 $B(1, *)$ には、データ $/D_N$ 内のブロックが交換されたデータ D_N が格納され、 $B(j, *)$ には、データ $/D_{N-j+1}$ 内のブロックが交換されたデータ D_{N-j+1} が格納され、 $B(N-j+1, 1 \sim M)$ には、データ $d_1 \sim d_M$ が格納され、 $B(N, *)$ には、データ $/D_1$ 内のブロックが交換されたデータ D_1 が格納される。

【0061】次いで、ステップS12からS15までを経て、各エリアに格納されているデータは、暗号化データの半分の位置 $N/2$ を対称にして交換される。したがって、図5(c)に示すように、 $B(1, *)$ には、データ D_1 が格納され、 $B(j, 1 \sim M)$ には、データ $d_1 \sim d_M$ が格納され、 $B(N-j+1, *)$ には、データ D_{N-j+1} が格納され、 $B(N, *)$ には、データ D_N が格納される。

【0062】すなわち、この暗号化データは、拡散されたエリアの配置が初期の状態に戻られるので、解読可能な元の平文データとなり、ステップS16において、補助記憶部5の所定領域に格納される。

【0063】このようにして、各エリアを対にして交換すれば、平文データを暗号化するときと同一の処理で、暗号化データを元の平文データに復号化することができる。このため、暗号化または復号化するためのデータ処理部とをそれぞれ個別に設計する必要がなく、暗号化/復号化ソフトを開発するために要する時間や費用、または手間などを大幅に削減することができる。

【0064】特に、各エリアをさらに複数のブロックに分割すれば、より解読困難な暗号化データを生成することができるだけでなく、各ブロックを対にする組み合わせが増大するから、それらの組み合わせを適宜に選択してバリエーションに富んだ暗号化/復号化ソフトを開発することができる。

【0065】さらに、対象データを各エリアが偶数個構成されるように分割すれば、各エリアは、必ず他のエリアと対にされて交換されるから、すべてのエリアの配置をもれなく拡散することができる。なお、エリアをブロックに分割する場合についても同様のことがいえる。

【0066】さらに、各エリア同士を交換する際に、そのエリアに格納されているデータを構成するビットを反転させれば、より解読困難な暗号化データを生成することができる。特に、上記処理は、分割したエリアの配置を拡散することを特徴としているため、平文データが文書データである場合に、分割するエリアの長さを大きく設定してしまうと、第三者がその生成された暗号化データを一瞥することによって、暗号化データの拡散規則が

解読される可能性があるが、このように、構成するすべてのビットを反転しておけば、その拡散規則を解読することが極めて困難となる。

【0067】次に、第2の実施の形態を説明する。この第2の実施の形態は、本発明に係るデータ変換装置を、分割した各エリアを対にする組み合わせに関する情報を暗号キーおよび復号キーとして用いて、平文データを暗号化し、または、暗号化データを復号化する場合について適用したものである。

【0068】このデータ変換装置は、上記第1の実施の形態における演算処理部3の構成を変更したものであって、演算処理部3は、補助記憶部5に格納されている平文データを暗号化し、または、暗号化データを復号化しようとするときには、図6のフローチャートに示す処理を実行するように構成されている。ここで、図6は、暗号キーによって平文データを暗号化し、または、復号キーによって暗号化データを復号化するための処理を示すフローチャートである。

【0069】つまり、平文データを暗号化し、または、暗号化データを復号化しようとするときに、演算処理部

$$0 \leq x < \prod_{i=1}^n (2N - 2i + 1) \quad (\text{式1})$$

次いで、ステップS25に移行して、処理回数を計数するための変数*i*に“1”を、対にするエリアの一方の位置を特定するための変数*A*に“1”を、フラグデータを格納するための変数*C* (1~*n*)に“0”を設定し、ステップS26に移行して、処理回数を計数するための変数*j*および*k*に“0”を設定し、ステップS27に移行して、変数*C* (*A* + *j* + *k*)の値が“0”であるか否かを判定し、“0”であると判定されたときには、ステップS28に移行する。

【0072】ステップS28では、変数*k*の値が“0”であるか否かを判定し、“0”であると判定されたときには、ステップS29に移行して、変数*A*の値に変数*j*の値を加算し、変数*j*の値に“0”を設定し、ステップS30に移行して、変数*k*の値に“1”を加算し、ステップS31に移行して、変数*k*の値が、変数*x*を(*n* - *i*)で除して得た余りに“1”を加算した値よりも大きいか否かを判定し、大きいと判定されたときには、ステップS32に移行する。

【0073】ステップS32では、バッファB (*A*)に格納されているデータとバッファB (*A* + *j* + *k* - 1)に格納されているデータとを交換し、ステップS33に移行して、変数*C* (*A*)と*C* (*A* + *j* + *k* - 1)とにそれぞれ“1”を設定する。

【0074】次いで、ステップS34に移行して、変数*x*に、変数*x*の値を(*n* - *i*)で除してその値を整数化したものを設定し、ステップS35に移行して、変数*i*の値が変数*n*の値よりも小さいか否かを判定し、小さく

3では、次のようにして処理を実行する。まず始めに、図6に示すように、ステップS21からS23までを経て、バッファBに補助記憶部5から対象データを読み込み、変数*n*に偶数の値をとるエリア数を設定し、バッファBを変数*n*が示す個数のエリアに分割する。ここで、変数*n*に設定するエリア数は、あらかじめ設定した固定の値を用いるものとする。なお、以降、対象データの先頭から*j* (1 ≤ *j* ≤ *n*) 番目のエリアに格納されているデータを示す場合には、B (*j*)と表記する。

【0070】次いで、ステップS24に移行して、変数*x*にエリアの配置を拡散するための暗号キーまたは復号キーとなるものをキーボード6から入力する。つまり、対象データをエリアが2*N*個構成されるように分割した場合、各エリアを対にする組み合わせの総数は、下式1の右辺に示すだけ存在することから、変数*x*には、これら組み合わせの一を特定する値を設定するようにする。すなわち、変数*x*には、下式1の条件を満たすような自然数を設定する。

【0071】

ないと判定されたときには、ステップS36に移行し、このように対象データのエリアの配置を拡散したものを、補助記憶部5の所定領域に格納して、一連の処理を終了する。

【0075】一方、ステップS27で、変数*C* (*A* + *j* + *k*)の値が“0”でないと判定されたときには、ステップS37に移行して、変数*j*の値に“1”を加算し、ステップS31に移行する。

【0076】また一方、ステップS28で、変数*k*の値が“0”でないと判定されたときには、ステップS30に移行する。また一方、ステップS31で、変数*k*の値が、変数*x*を(*n* - *i*)で除して得た余りに“1”を加算した値よりも大きくないと判定されたときには、ステップS27に移行する。

【0077】また一方、ステップS35で、変数*i*の値が変数*n*の値よりも小さいと判定されたときには、ステップS26に移行する。次に、上記第2の実施の形態の動作を図面を参照しながら説明する。図7は、暗号キーの値に応じて平文データを暗号化する場合を説明するブロック図である。

【0078】ここでは、平文データを4つのエリアに分割したときに、入力する暗号キーの値に応じて、それらエリアを対にする組み合わせを決定する場合について説明する。なお、ステップS21からS23までを経て、平文データを4つのエリアに分割したときに、B (1~4)には、それぞれデータ*d*₁ ~ *d*₄ が格納されているものとする。

【0079】まず、分割するエリア数は4つであるので、上式1の右辺により、各エリアを対にする組み合わせの総数は、“3”と算出される。このとき、暗号キーとしての変数 x に設定し得る値の範囲は、上式1より“0”～“2”である。

【0080】そこで、送信者は、暗号キーとしての変数 x に“0”を入力するものとする、ステップS25からS29までを経て、変数 A には、変数 A の値“1”と変数 j の値“0”とを加算した値“1”が設定され、ステップS30からS31までを経て、変数 k の値“1”が“1”（変数 x の値“0”を“3”で除して得た余り“0”に“1”を加算した値）よりも大きくないので、ステップS27からS28まで、ステップS30からS31までを経て、変数 k の値“2”が“1”よりも大きくなったときに、ステップS32に処理が移行される。

【0081】このとき、変数 j 、 k 、 A の値は、それぞれ“0”、“2”、“1”であるので、ステップS32からS34までを経て、 $B(1)$ に格納されているデータ d_1 と $B(2)$ に格納されているデータ d_2 とが交換され、変数 $C(1)$ と $C(2)$ とに“1”が、変数 x に“0”が設定される。

【0082】次いで、ステップS26に処理が戻され、変数 $C(1)$ および $C(2)$ の値が“1”であるので、変数 j の値が“2”となるが、ステップS29において、変数 A の値“1”に変数 j の値が“2”が加算されたときに、変数 j には、“0”が設定され、ステップS32に処理が移行される。

【0083】このとき、変数 j 、 k 、 A の値は、それぞれ“0”、“2”、“3”であるので、ステップS32からS36までを経て、 $B(3)$ に格納されているデータ d_3 と $B(4)$ に格納されているデータ d_4 とが交換される。

【0084】すなわち、図7の上段に示すように、 d_1 、 d_2 、 d_3 、 d_4 の順序で構成されていた平文データは、 d_2 、 d_1 、 d_4 、 d_3 の順序で並び換えられた暗号化データとなる。

【0085】次に、送信者は、暗号キーとしての変数 x に“1”を入力するものとする、ステップS27からS31までを3回繰り返したのちに、ステップS32に処理が移行される。このとき、変数 j 、 k 、 A の値は、それぞれ“0”、“3”、“1”であるので、ステップS32からS34までを経て、 $B(1)$ に格納されているデータ d_1 と $B(3)$ に格納されているデータ d_3 とが交換され、変数 $C(1)$ と $C(3)$ とに“1”が、変数 x に“0”が設定される。

【0086】次いで、ステップS27からS31までを2回繰り返したのちに、ステップS32に処理が移行される。このとき、変数 j 、 k 、 A の値は、それぞれ“1”、“2”、“2”であるので、ステップS32からS36までを経て、 $B(2)$ に格納されているデータ

d_2 と $B(4)$ に格納されているデータ d_4 とが交換される。すなわち、図7の中段に示すように、 d_1 、 d_2 、 d_3 、 d_4 の順序で構成されていた平文データは、 d_3 、 d_4 、 d_1 、 d_2 の順序で並び換えられた暗号化データとなる。

【0087】次に、送信者は、暗号キーとしての変数 x に“2”を入力するものとする、ステップS27からS31までを4回繰り返したのちに、ステップS32に処理が移行される。このとき、変数 j 、 k 、 A の値は、それぞれ“0”、“4”、“1”であるので、ステップS32からS34までを経て、 $B(1)$ に格納されているデータ d_1 と $B(4)$ に格納されているデータ d_4 とが交換され、変数 $C(1)$ と $C(4)$ とに“1”が、変数 x に“0”が設定される。

【0088】次いで、ステップS27からS31までを2回繰り返したのちに、ステップS32に処理が移行される。このとき、変数 j 、 k 、 A の値は、それぞれ“0”、“2”、“2”であるので、ステップS32からS36までを経て、 $B(2)$ に格納されているデータ d_2 と $B(3)$ に格納されているデータ d_3 とが交換される。

【0089】すなわち、図7の下段に示すように、 d_1 、 d_2 、 d_3 、 d_4 の順序で構成されていた平文データは、 d_4 、 d_3 、 d_2 、 d_1 の順序で並び換えられた暗号化データとなる。

【0090】なお、これらの暗号化データは、暗号化したときに変数 x に入力した値と同一の値を入力すれば、解読可能な元の平文データに復号化される。このようにして、分割した各エリアを対にする組み合わせに関する情報を定量的にすれば、通常の暗号化技術のように暗号キー／復号キーを用いるようにした場合であっても、平文データを暗号化するときと同一の処理で、暗号化データを元の平文データに復号化することができる。

【0091】なお、上記第1の実施の形態においては、各エリアをさらに複数のブロックに分割するように構成した場合について説明したが、これに限らず、各エリアを複数のブロックに分割しないように構成してもよい。

【0092】また、上記第1の実施の形態においては、エリアを交換する際に、そのエリアに格納されているデータを構成するビットを反転させるように構成した場合について説明したが、これに限らず、ビットを反転させないように構成してもよい。

【0093】さらに、上記第1の実施の形態においては、各エリアおよびブロックをそれぞれ一度だけ交換するように構成した場合について説明したが、これに限らず、すべてのエリアおよびブロックを必ず1度だけ交換するという処理を単位交換処理とし、各単位交換処理ごとに、対にするエリアの組み合わせを異ならせて、これを複数回実行するように構成してもよい。

【0094】さらに、上記第1の実施の形態において

は、暗号キー／復号キーを用いないで構成した場合について説明したが、これに限らず、例えば、エリアの分割個数Nまたはブロックの分割個数Mを暗号キーおよび復号キーとして用いるように構成してもよい。

【0095】さらに、上記第1の実施の形態においては、ブロック同士を交換してから、エリア同士を交換するように構成した場合について説明したが、これに限らず、エリア同士を交換してから、ブロックを交換するように構成してもよい。

【0096】さらに、上記第1の実施の形態においては、各エリアをさらに複数のブロックに分割した2段階の構成について説明したが、これに限らず、ブロックをさらに複数の微小なブロックに分割する3段階の構成にしたり、多段階の構成にしたりするのであってもよい。

【0097】さらに、上記第2の実施の形態においては、各エリアをさらに複数のブロックに分割しないように構成した場合について説明したが、これに限らず、各エリアを複数のブロックに分割するように構成してもよい。

【0098】さらに、上記第2の実施の形態においては、エリアを交換する際に、そのエリアに格納されているデータを構成するビットを反転させないように構成した場合について説明したが、これに限らず、ビットを反転させるように構成してもよい。

【0099】さらに、上記実施の形態においては、各エリアまたは各ブロックが偶数個構成されるように分割した場合について説明したが、これに限らず、それらが奇数個構成されるように分割してもよい。そうすると、すべてのエリアまたはブロックのうち、一つだけ交換されないエリアまたはブロックが存在してしまうが、対象データを膨大な数のエリアが構成されるように分割し、さらに、そのエリアも膨大な数のブロックが構成されるように分割すれば、一つだけ交換されていないエリアまたはブロックを発見することが極めて困難となるので、特に問題は生じない。

【0100】さらに、上記実施の形態においては、エリアに格納されているデータを構成するすべてのビットを反転させるように構成した場合について説明したが、これに限らず、あらかじめ設定した特定のビットのみを反転させるように構成してもよい。このようにすれば、例えば、ビットを反転させる位置を特定する情報を暗号キー／復号キーとして用いることもできる。

【0101】さらに、上記実施の形態において、演算処理部3で、図3および図6のフローチャートに示す処理を実行するにあたっては、主記憶部4にあらかじめ格納されているプログラムを実行する場合について説明したが、これに限らず、これらの手順を示したプログラムが記録された記録媒体から、そのプログラムを主記憶部4に読み込んで実行するようにしてもよい。ここで、記録媒体とは、RAM、ROM、FD、コンパクトディス

ク、ハードディスクまたは光磁気ディスク等の記録媒体であって、電子的、磁氣的、光学的等の記録方法のいかんを問わず、コンピュータで読み取り可能な記録媒体であれば、あらゆる記録媒体を指しているものである。

【0102】さらに、上記実施の形態において、図3および図6のフローチャートに示す処理は、ソフトウェアで構成した場合について説明したが、これに代えて、比較回路、演算回路、論理回路等の電子回路を組み合わせるように構成してもよい。

【0103】上記実施の形態において、ステップS2およびS3、または、ステップS22およびS23は、請求項1、2、4または5記載のデータ分割手段に対応し、ステップS13、または、ステップS32は、請求項1または3記載のエリア交換手段に対応し、ステップS4、S7、S10およびS11は、請求項3または4記載のエリア交換手段に対応し、上記単位交換処理を複数回実行する処理は、請求項3記載のエリア交換手段に対応している。

【0104】また、上記実施の形態において、ステップS6は、請求項6記載のビット反転手段に対応し、キーボード6およびステップS24は、請求項7記載の特定キー入力手段に対応し、ステップS25からS35までは、請求項7記載のエリア交換手段に対応している。

【0105】

【発明の効果】以上説明したように、本発明に係るデータ変換装置によれば、暗号化データを生成するときと同一の処理で、その暗号化データを復号化することができるから、暗号化／復号化ソフトを開発するために要する時間や費用、または手間などを大幅に削減することができるとともに、コンパクトなサイズの暗号化／復号化ソフトを開発することができるという効果が得られる。

【0106】さらに、本発明に係る請求項4記載のデータ変換装置によれば、エリアをさらに細分化することによって、各ブロックを対にする組み合わせが増大するから、それらの組み合わせを適宜に選択してバリエーションに富んだ暗号化／復号化ソフトを開発することができるという効果も得られる。

【0107】さらに、本発明に係る請求項2、4、5または6記載のデータ変換装置によれば、より解読困難な暗号化データを生成することができるという効果も得られる。

【0108】さらに、本発明に係る請求項2または5記載のデータ変換装置によれば、すべてのエリアまたはブロックの配置をもれなく拡散することができるという効果も得られる。

【0109】さらに、本発明に係る請求項7記載のデータ変換装置によれば、通常の暗号化技術のように暗号キー／復号キーを用いるようにした場合であっても、暗号化データを生成するときと同一の処理で、その暗号化データを復号化することができるという効果も得られる。

【図面の簡単な説明】

【図1】第1の実施の形態の構成を示すブロック図である。

【図2】第1の実施の形態におけるコンピュータ1a、1bの構成を示すブロック図である。

【図3】データを暗号化または復号化するための処理を示すフローチャートである。

【図4】平文データを暗号化する場合を説明するためのブロック図である。

【図5】暗号化データを復号化する場合を説明するためのブロック図である。

【図6】暗号キー／復号キーを用いてデータを暗号化または復号化するための処理を示すフローチャートである。

る。

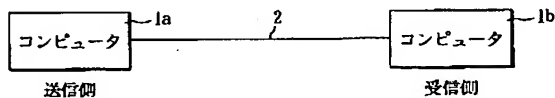
【図7】暗号キーの値に応じて平文データを暗号化する場合を説明するためのブロック図である。

【図8】従来のデータ変換装置におけるデータの処理過程を示すブロック図である。

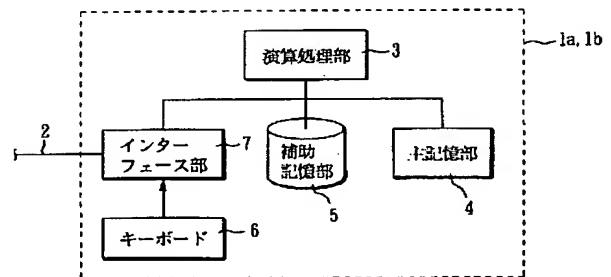
【符号の説明】

- 1 a, 1 b コンピュータ
- 2 データ伝送路
- 3 演算処理部
- 4 主記憶部
- 5 補助記憶部
- 6 インターフェース部
- 7 キーボード

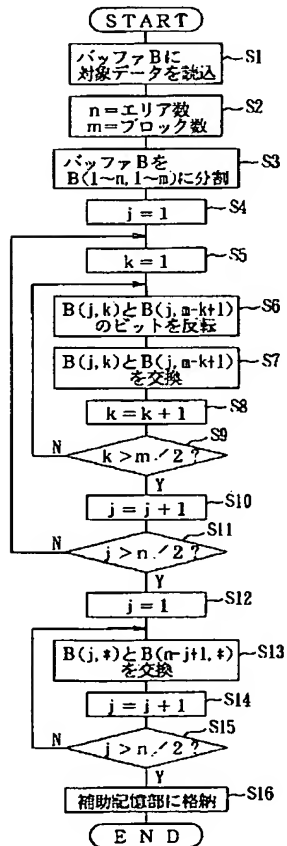
【図1】



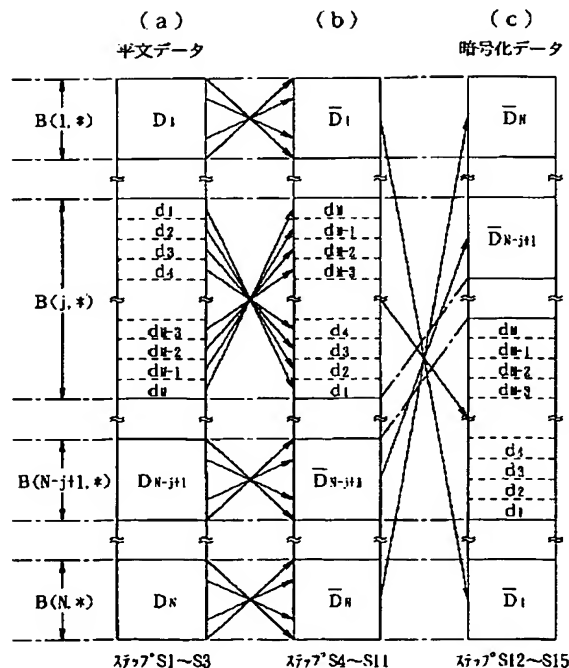
【図2】



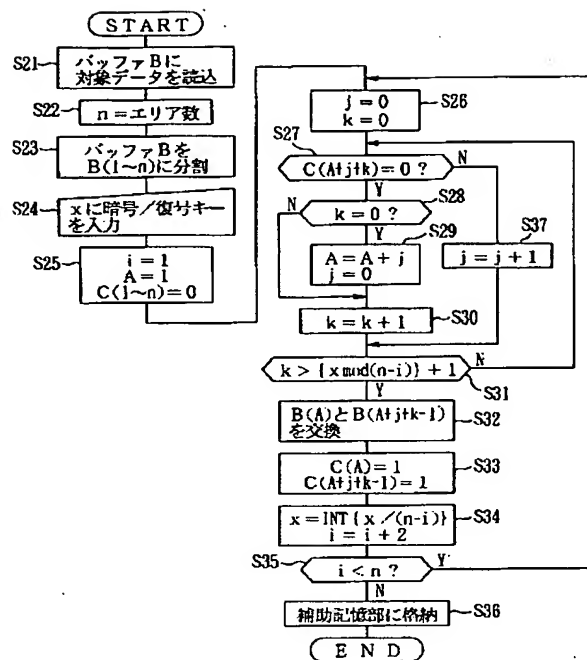
【図3】



【図4】



【図 6】



【図 7】

暗号キー X	平文データ	交換する組み合わせ	暗号化データ
	B(1) B(2) B(3) B(4)	B(1) B(2) B(3) B(4)	B(1) B(2) B(3) B(4)
0	d ₁ d ₂ d ₃ d ₄	<div style="display: flex; justify-content: space-around;"> d₁ d₂ d₃ d₄ </div>	d ₂ d ₁ d ₄ d ₃
1	d ₁ d ₂ d ₃ d ₄	<div style="display: flex; justify-content: space-around;"> d₁ d₂ d₃ d₄ </div>	d ₃ d ₄ d ₁ d ₂
2	d ₁ d ₂ d ₃ d ₄	<div style="display: flex; justify-content: space-around;"> d₁ d₂ d₃ d₄ </div>	d ₄ d ₃ d ₂ d ₁

【図8】

